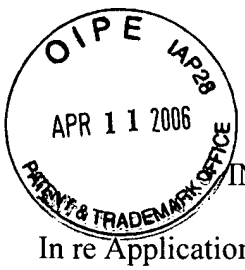
AT-2134/188 ZW



PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:
Geoffrey S. Strongin

Serial No.: 09/853,465

Filed: May 11, 2001

For: CRYPTOGRAPHIC COMMAND-RESPONSE ACCESS TO A MEMORY IN A PERSONAL COMPUTER SYSTEM

Examiner: E. TRAN

Group Art Unit: 2134

Att'y Docket: 2000.039500

Customer No. 023720

APPEAL BRIEF

CERTIFICATE OF MAILING
37 C.F.R. 1.8

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date below:

04/07/06 Kathy Klauer
Date Signature

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby submits this Appeal Brief to the Board of Patent Appeals and Interferences in response to the final Office Action dated November 15, 2005. A Notice of Appeal was filed on February 14, 2006 and so this Appeal Brief is believed to be timely filed.

It is believed that a fee of $500.00 is due. A check is enclosed. However, should the check be inadvertently omitted, the Commissioner is authorized to deduct the fee for filing this Appeal Brief ($500) from Williams, Morgan & Amerson, P.C.'s Deposit 50-0786/2000.039500.

04/11/2006 HDESTA1 00000085 09853465
01 FC:1402 500.00 OP

I. REAL PARTY IN INTEREST

The present application is owned by Advanced Micro Devices, Inc. The assignment of the present application to Advanced Micro Devices, Inc., is recorded at Reel 11804, Frame 0899.

II. RELATED APPEALS AND INTERFERENCES

Applicant is not aware of any related appeals and/or interferences that might affect the outcome of this proceeding.

III. STATUS OF THE CLAIMS

Claims 1-103 are pending in the present application. Claims 1-103 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the enablement requirement. Claims 1-103 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Claims 1-103 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Vu, et al (U.S. Patent No. 6,557,104).

IV. STATUS OF AMENDMENTS

There were no amendments after the final rejections.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1, 55, and 62 sets forth reading a secret from a first location, securing the secret in a secure location different from the first location, and retrieving at least a portion of the data stored in the first location using the secret. For example, the method 3620 shown in Fig. 27

includes storing a secret in a storage device (block 3805). The storage device may include only a portion of a physical device. The method 3620 may also include storing data in the storage device (block 3810) and storing code in the storage device (block 3815). The method 3620 may also include providing a lock (*e.g.* a lock bit or bits) to secure data stored in the storage device or the storage device itself (block 3815). The method 3620 also includes reading the secret from the storage device (block 3825), such as, for example, when the computer system including the storage device or coupled to communicate with the storage device is booted. For the secret to remain secure, the reading of the secret preferably occurs when the storage device is in a secure or trusted configuration. The method 3620 may also read the code from the storage device (block 3830). The method 3620 stores the secret in a secure location (block 3825) and also may store the code in the secure location (block 3830). The secure location may be in the SMM memory space previously described, or in a secure memory, register, or other storage location in the computer system 100, such as in the processor 805 or in the south bridge 330. See Patent Application, page 71, line 17 – page 72, line 10.

Claim 51 sets forth a personal computer system including means for securely storing data, means for reading a secret from the means for securely storing data, means for securing the secret in a secure location different from the means for securely storing data, and means for retrieving at least a portion of the data stored in the means for securely storing data using the secret. For example, Fig. 7C illustrates an embodiment of protected storage 605, according to one aspect of the present invention. As shown, protected storage 605 is coupled to the LPC bus 118 and includes logic 609 and secret 610B, in addition to its storage locations. The protected storage 605 may include memory, such as RAM, ROM, flash memory, etc., or other storage media, such as hard drives, CDROM storage, etc. Although shown as a single unit, the protected

storage is also contemplated as a sub-system that includes separate components for storage and logic, such as shown in Fig. 7D. According to Fig. 7D, a crypto-processor 305, including a secret 610A, is coupled in front of a protected storage 605B. Access to the protected storage 605B is through the crypto-processor 305. The protected storage 605B includes data storage 608A, access logic 609B, a lock register 606, and code storage 607, including a secret 610B. See Patent Application, page 31, ll. 9-19.

Claims 32, 64, and 97 set forth storing a secret within a first location and storing code different from the secret within the first location, where the code is configured to provide access to data stored in the first location when processed in association with the secret. Fig. 27, the method 3620 includes storing a secret in a storage device (block 3805). The method 3620 may also include storing data in the storage device (block 3810) and storing code in the storage device (block 3815). The method 3620 also includes reading the secret from the storage device (block 3825), such as, for example, when the computer system including the storage device or coupled to communicate with the storage device is booted. For the secret to remain secure, the reading of the secret preferably occurs when the storage device is in a secure or trusted configuration. The method 3620 may also read the code from the storage device (block 3830). The method 3620 stores the secret in a secure location (block 3825) and also may store the code in the secure location (block 3830). The secure location may be in the SMM memory space previously described, or in a secure memory, register, or other storage location in the computer system 100, such as in the processor 805 or in the south bridge 330. See Patent Application, page 71, line 17 – page 72, line 10.

Claim 39 sets forth a first location configured to store code, a secret, and data different from the secret and different from the code, and a master device operably coupled to the first

location, wherein the master device is configured to read the secret from the first location and to store the secret in a secure location different from the first location, and wherein the master device is further configured to access the data stored in the first location using the secret. For example, Fig. 7C illustrates an embodiment of protected storage 605, according to one aspect of the present invention. As shown, protected storage 605 is coupled to the LPC bus 118 and includes logic 609 and secret 610B, in addition to its storage locations. The protected storage 605 may include memory, such as RAM, ROM, flash memory, etc., or other storage media, such as hard drives, CDROM storage, etc. Although shown as a single unit, the protected storage is also contemplated as a sub-system that includes separate components for storage and logic, such as shown in Fig. 7D. According to Fig. 7D, a crypto-processor 305, including a secret 610A, is coupled in front of a protected storage 605B. Access to the protected storage 605B is through the crypto-processor 305. The protected storage 605B includes data storage 608A, access logic 609B, a lock register 606, and code storage 607, including a secret 610B. See Patent Application, page 31, ll. 9-19.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Appellant respectfully requests that the Board review and overturn the three rejections present in this case. The following issues are presented on appeal in this case:

(A) Whether claims 1-103 fail to comply with the enablement requirement;

(B) Whether claims 1-103 are indefinite; and

(C) Whether claims 1-103 are anticipated by Vu.

VII. ARGUMENT

A. Legal Standards

The test for determining compliance with the written description requirement is whether the disclosure of the application as originally filed reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter, rather than the presence or absence of literal support in the specification for the claim language. *In re Edwards*, 558 [568] F.2d 1349, 196 USPQ 465 (CCPA 1978); *In re Herschler*, 591 F.2d 693, 200 USPQ 711 (CCPA 1979); *In re Kaslow*, 707 F.2d 1366, 217 USPQ 1089 (Fed. Cir. 1983). The content of the drawings may also be considered in determining compliance with the written description requirement. *In re Barker*, 559 F.2d 588, 194 USPQ 470 (CCPA 1977); *In re Kaslow*, 707 F.2d 1366, 217 USPQ 1089 (Fed. Cir. 1983).

The test of enablement is whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation. *United States vs. Telectronics, Inc.*, 857 F.2d 778, 785 8 USPQ2d 1217, 1223 (Fed. Cir. 1998). A patent need not teach, and preferably omits, what is well known in the art. *In re Buchner*, 929 F.2d 660, 661, 18 USPQ2d 1331, 1332 (Fed. Cir. 1991).

An anticipating reference by definition must disclose every limitation of the rejected claim in the same relationship to one another as set forth in the claim. *In re Bond*, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990).

B. Claims 1-103 comply with the enablement requirement.

The Examiner alleges that specification does not describe what data or secret is stored in the first location and therefore the Examiner alleges that the use of a secret is not enabled.

Applicant respectfully disagrees and submits that the use of secret information to protect confidential information is well-known. Furthermore, the secret information may take a variety of forms. Support for this position may be found in the references cited by the Examiner. *See, e.g.*, Vu, col. 1, ll. 11-33. Thus, Applicant respectfully submits that one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation.

Applicant therefore submits that the specification does enable the use of a secret and requests that the Examiner's rejections of claim 1-103 under 35 U.S.C. § 112, first paragraph, be REVERSED.

C. Claims 1-103 are definite.

The Examiner alleges that specification does not describe what data or secret is stored in the first location and therefore the Examiner alleges that the claims are indefinite. Applicant disagrees and respectfully submits that the use of secret information to protect confidential information is well-known. Furthermore, the secret information may take a variety of forms. Support for this position may be found in the references cited by the Examiner. *See, e.g.*, Vu, col. 1, ll. 11-33. Moreover, Applicant respectfully submits that it is not necessary to set forth particular examples of secrets to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

The Examiner also alleges that the specification does not explain what function or uses are performed when retrieving the data from the first location. Applicant respectfully submits that some embodiments of the present invention set forth techniques for accessing data stored in

a first location using a secret. The contents and/or the function of the accessed data are not material to the present invention.

For at least the aforementioned reasons, Applicant respectfully submits that the disclosure of the application as originally filed reasonably conveys to the artisan that the inventor had possession at that time of the later claimed subject matter. Applicant therefore submits that the claims are definite and requests that the Examiner's rejections of claim 1-103 under 35 U.S.C. § 112, second paragraph, be REVERSED.

D. Claims 1-103 are not anticipated by Vu.

Vu describes storing a cryptographic key, as well as a cryptographic program and any other data or information that may be required for the cryptographic processing, on a token, such as a magnetic strip, PCMCIA card, floppy disk, CD ROM, or any other similar removable storage device. See Vu, col. 4, ll. 21-36. The cryptographic key, the cryptographic program and other related data stored on the token may be loaded into a System Management RAM (SMRAM) and the SMRAM is then locked to prevent any other processes from accessing the data stored in the SMRAM. See Vu, col. 4, ll. 52-54. Once the cryptographic key has been stored in the SMRAM, the physical token is removed to ensure system integrity. See Vu, Col. 5, ll. 10-12. A security function may access the cryptographic key and programs stored in the SMRAM to perform security processing. See Vu, col. 5, ll. 35-37.

However, Applicant respectfully submits that Vu fails to teach or suggest reading a secret from a first location, securing the secret in a secure location different from the first location, and retrieving at least a portion of the data stored in the first location using the secret, as set forth in independent claims 1, 51, 55, and 66. Although Vu describes transferring a cryptographic

program (and any other data or information that may be required for the cryptographic processing) from the physical token to the SMRAM, Vu does not teach that the cryptographic key is used to access the cryptographic program or any other data or information that may be stored on the physical token. To the contrary, the physical token that originally stored the cryptographic key must be removed to ensure system integrity, thereby preventing the system from accessing any data stored on the physical token after the cryptographic key has been transferred to the SMRAM.

In the Final Office Action, the Examiner confirms the above analysis of Vu. First, the Examiner identifies the physical token as the "first location." Second, the Examiner identifies the SMRAM as the "secure location different than the first location." See Final Office Action, page 4. Third, the Examiner states that the data is accessed from the SMRAM, *i.e.*, the "secure location different than the first location," using the cryptographic key. See Final Office Action, page 5. Thus, Vu does not teach that the cryptographic key is used to access the cryptographic program or any other data or information that may be stored on the physical token. To the contrary, the cryptographic key is used to access information from the SMRAM and not from the physical token, *i.e.*, the "first location" identified by the Examiner. In fact, it is impossible to access information stored on the physical token because the physical token is removed to ensure system integrity once the cryptographic key has been stored in SMRAM.

Applicant also submits that Vu fails to teach or suggest storing a secret within a first location and storing code different from the secret within the first location, where the code is configured to provide access to data stored in the first location when processed in association with the secret, as set forth in independent claims 32, 64, and 97.

Applicant also submits that Vu fails to teach or suggest a first location configured to store code, a secret, and data different from the secret and different from the code, and a master device operably coupled to the first location, wherein the master device is configured to read the secret from the first location and to store the secret in a secure location different from the first location, and wherein the master device is further configured to access the data stored in the first location using the secret, as set forth in independent claim 39.

For at least the aforementioned reasons, Applicant respectfully submits that the present invention is not anticipated by Vu and requests that the Examiner's rejections of claims 1-103 under 35 U.S.C. 102(e) be REVERSED

VIII. CLAIMS APPENDIX

The claims that are the subject of the present appeal – claims 1-103 – are set forth in the attached "Claims Appendix."

IX. EVIDENCE APPENDIX

There is no separate Evidence Appendix for this appeal.

X. RELATED PROCEEDINGS APPENDIX

There is no Related Proceedings Appendix for this appeal.

XI. CONCLUSION

In view of the foregoing, it is respectfully submitted that the Examiner erred in not allowing all claims pending in the present application, claims 1-103, over the prior art of record.

The undersigned may be contacted at (713) 934-4052 with respect to any questions, comments or suggestions relating to this appeal.

Respectfully submitted,

Date: 4/7/06

Mark W. Sincell, Ph.D.
Reg. No. 52,226
WILLIAMS, MORGAN & AMERSON
10333 Richmond, Suite 1100
Houston, Texas 77042
(713) 934-7000
(713) 934-7011 (facsimile)

AGENT FOR APPLICANTS

CLAIMS APPENDIX

1. A method of securely accessing data in a personal computer, the method comprising:

reading a secret from a first location;

securing the secret in a secure location different from the first location; and

retrieving at least a portion of the data stored in the first location using the secret.

2. The method of claim 1, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory; and

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret.

3. The method of claim 2, wherein the memory is a read-only memory (ROM);

wherein reading a secret from the memory comprises reading the secret from the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in the secure location different from the ROM; and

wherein retrieving at least a portion of the data stored in the memory using the secret comprises retrieving at least the portion of the data stored in the ROM using the secret.

4. The method of claim 3, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM;

wherein securing the secret in the secure location different from the ROM comprises securing the secret in the secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data stored in the ROM using the secret comprises retrieving at least a portion of the BIOS data stored in the BIOS ROM using the secret.

5. The method of claim 3, wherein reading the secret from the ROM comprises reading the secret from within the data stored within the ROM.

6. The method of claim 1, further comprising:

reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location;

wherein retrieving at least a portion of the data stored in the first location using the secret comprises retrieving at least a portion of the data stored in the first location using the code and the secret.

7. The method of claim 6, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory; and

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret.

8. The method of claim 7, wherein reading the secret within the memory and reading code from the memory further comprises reading the secret from inside the code within the memory.

9. The method of claim 6, further comprising:

unlocking a lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

10. The method of claim 9, wherein the location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret; and

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

11. The method of claim 9, further comprising:

processing the secret using the code;

wherein unlocking a lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the first location in response to processing the secret using the code.

12. The method of claim 11, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory, wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret;

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking the lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the memory in response to processing the secret using the code.

13. The method of claim 1, further comprising:

unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

14. The method of claim 13, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises

unlocking a lock bit associated with data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

15. The method of claim 1, further comprising:

storing the secret within the first location securely;

storing data within the first location securely; and

storing code different from the secret and different from the data within the first location securely.

16. The method of claim 15, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein storing the secret within the first location securely comprises storing the secret within the memory securely;

wherein storing data within the first location securely comprises storing data within the memory securely; and

wherein storing code different from the secret and different from the data within the first location securely comprises storing code different from the secret and different from the data within the memory securely

17. The method of claim 16, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM;

wherein storing data within the memory comprises storing data within the ROM;

wherein storing code different from the secret and different from the data within the memory comprises storing code different within secret and different from the data within the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in a secure location different from the ROM; and

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the ROM using the secret.

18. The method of claim 17, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing data within the ROM comprises storing data within the BIOS ROM;

wherein storing code different within secret and different from the data within the ROM comprises storing code different within secret and different from the BIOS data within the BIOS ROM;

wherein securing the secret in a secure location different from the ROM comprises securing the secret in a secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data from the ROM using the secret comprises retrieving at least a portion of the BIOS data from the BIOS ROM using the secret.

19. The method of claim 16, wherein storing a secret within the memory and storing data within the memory comprises storing the secret inside the data within the memory.

20. The method of claim 16, wherein storing a secret within the memory and storing code different from the secret and different from the data within the memory comprises storing the secret inside the code within the memory.

21. The method of claim 16, further comprising:

unlocking a lock bit associated with the data prior to retrieving at least the portion of the data from the memory using the secret.

22. The method of claim 21, further comprising:

reading the code from the memory; and

securing the code in a secure location different from the memory;

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the memory using the code and the secret.

23. The method of claim 22, wherein reading the secret from the memory comprises reading the secret from the memory during a boot sequence; and

wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

24. The method of claim 22, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

processing the code; and

transmitting at least an indication of the secret to the memory;

25. The method of claim 24, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

receiving a challenge from the memory; and

transmitting a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

26. The method of claim 1, further comprising:

reading the code from the first location; and

securing the code in a secure location different from the first location;

wherein retrieving at least a portion of the data from the first location using the secret comprises retrieving at least a portion of the data from the first location using the code and the secret.

27. The method of claim 26, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading the code from the reading the code from the memory comprises reading the code from the memory;

wherein securing the code in a secure location different from the first location comprises securing the code in a secure location different from the memory; and

wherein retrieving at least a portion of the data from the first location using the secret further comprises retrieving at least a portion of the data from the memory using the code and the secret.

28. The method of claim 1, wherein reading the secret from the first location comprises reading the secret from the first location during a boot sequence; and

wherein securing the secret in a secure location different from the first location comprises storing the secret in SMM memory space.

29. The method of claim 28, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein reading the secret from the memory further comprises reading the secret from the memory during a boot sequence.

30. The method of claim 1, further comprising:

providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured.

31. The method of claim 30, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein providing the lock bit associated with the data that when set provides an indication that the data stored in the first location is secured comprises providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured

32. A method of securing data in a personal computer system, the method comprising:

storing a secret within a first location; and

storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

33. The method of claim 32, wherein the first location comprises a memory;

wherein storing the secret within the first location comprises storing a secret within the memory;

wherein storing code different from the secret within the first location comprises storing code different from the secret within the memory; and

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret further comprises the code being configured to provide access to data stored in the memory when processed in association with the secret.

34. The method of claim 33, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM; and

wherein storing code different from the secret within the memory comprises storing code different within secret within the ROM; and

wherein the code is configured to provide access to data stored in the ROM when processed in association with the secret.

35. The method of claim 34, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing code different within secret within the ROM comprises storing code different within secret within the BIOS ROM; and

wherein the code is configured to provide access to BIOS data stored in the BISO ROM when processed in association with the secret.

36. The method of claim 33, wherein storing a secret within the memory comprises storing the secret inside the data within the memory.

37. The method of claim 33, wherein storing a secret within the memory and storing code different from the secret within the memory comprises storing the secret inside the code within the memory.

38. The method of claim 33, further comprising:

providing a lock bit associated with the data stored in the memory that when set provides an indication that the data stored in the memory is secured.

39. A personal computer system, comprising:

a first location configured to store code, a secret, and data different from the secret and different from the code;

a master device operably coupled to the first location, wherein the master device is configured to read the secret from the first location and to store the secret in a secure location different from the first location, and wherein the master device is further configured to access the data stored in the first location using the secret.

40. The personal computer system of claim39, wherein the first location comprises a memory.

41. The personal computer system of claim 40, wherein the memory comprises a read-only memory (ROM).

42. The personal computer system of claim 41, wherein the ROM comprises a basic input-output system (BIOS) ROM, and wherein the data comprise BIOS data.

43. The personal computer system of claim 41, wherein the master device is further configured to read the secret from within the data stored within the ROM.

44. The computer system of claim 41, wherein the master device is further configured to read the code from the memory; and wherein the master device is further configured to retrieve at least a portion of the data stored in the memory using the code and the secret.

45. The computer system of claim 39, further comprising:

a lock bit associated with the data stored in the first location; and

wherein the master device is further configured to unlock the lock bit associated with the data stored in the first location.

46. The personal computer system of claim 45, wherein the first location comprises a memory.

47. The computer system of claim 46, wherein the master device is further configured to process the secret using the code; and wherein the master device is further configured to unlock the lock bit associated with the data stored in the memory in response to processing the secret using the code.

48. The computer system of claim 47, wherein the master device is further configured to receive a challenge from the memory and to transmit a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

49. The computer system of claim 39, wherein the master device is further configured to read the secret from the first location during a boot sequence; and wherein the master device is further configured to store the secret in SMM memory space.

50. The computer system of claim 39, wherein the master device includes a microprocessor.

51. A personal computer system, comprising:

means for securely storing data;

means for reading a secret from the means for securely storing data;

means for securing the secret in a secure location different from the means for securely storing data; and

means for retrieving at least a portion of the data stored in the means for securely storing data using the secret.

52. The personal computer system of claim 51, further comprising:

means for reading code from the means for securely storing data, wherein the code is different from the secret and different from the data stored in the means for securely storing data;

wherein the means for retrieving at least a portion of the data stored in the means for securely storing data from the means for securely storing data using the secret comprises means for retrieving at least a portion of the data stored in the means for securely storing data using the code and the secret.

53. The personal computer system of claim 51, further comprising:

means for locking the means for securely storing data; and

means for unlocking the means for locking.

54. The personal computer system of claim 51, further comprising:

means for processing the secret using the code.

55. A method of securely accessing data in a personal computer, the method comprising:

step for reading a secret from a first location;

step for securing the secret in a secure location different from the first location; and

step for retrieving at least a portion of the data stored in the first location using the secret.

56. The method of claim 55, further comprising:

step for reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location;

wherein the step for retrieving at least the portion of the data stored in the first location using the secret comprises step for retrieving at least the portion of the data stored in the first location using the code and the secret.

57. The method of claim 55, further comprising:

step for unlocking a lock bit associated with the data stored in the first location prior to the step for retrieving at least the portion of the data stored in the first location using the secret.

58. The method of claim 57, further comprising:

step for processing the secret using the code;

wherein the step for unlocking the lock bit associated with the data stored in the first location comprises step for unlocking the lock bit associated with the data stored in the first location in response to the step for processing the secret using the code.

59. The method of claim 55, further comprising:

step for storing the secret within the first location securely;

step for storing data within the first location securely; and

step for storing code different from the secret and different from the data within the first location securely.

60. The method of claim 59, further comprising:

step for unlocking a lock bit associated with the data prior to the step for retrieving at least the portion of the data from the first location using the secret.

61. The method of claim 60, further comprising:

step for reading the code from the first location; and

step for securing the code in a secure location different from the first location;

wherein the step for retrieving at least the portion of the data from the first location using the secret comprises step for retrieving at least the portion of the data from the first location using the code and the secret.

62. The method of claim 55, further comprising:

step for reading the code from the first location; and

step for securing the code in a secure location different from the first location;

wherein the step for retrieving at least the portion of the data from the first location using the secret comprises step for retrieving at least a portion of the data from the first location using the code and the secret.

63. The method of claim 55, further comprising:

step for providing a lock bit associated with the data that when set provides an indication that the data stored in the first location is secured.

64. A method of securing data in a personal computer system, the method comprising:

step for storing a secret within a first location; and

step for storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

65. The method of claim 64, further comprising:

step for providing a lock bit associated with the data stored in the first location that when set provides an indication that the data stored in the first location is secured.

66. A computer readable program storage device encoded with instructions that, when executed by a personal computer, performs a method of securely accessing data in the personal computer, the method comprising:

reading a secret from a first location;

securing the secret in a secure location different from the first location; and

retrieving at least a portion of the data stored in the first location using the secret.

67. The computer readable program storage device of claim 66, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory; and

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret.

68. The computer readable program storage device of claim 67, wherein the memory is a read-only memory (ROM);

wherein reading a secret from the memory comprises reading the secret from the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in the secure location different from the ROM; and

wherein retrieving at least a portion of the data stored in the memory using the secret comprises retrieving at least the portion of the data stored in the ROM using the secret.

69. The computer readable program storage device of claim 68, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein reading the secret from the ROM comprises reading the secret from the BIOS ROM;

wherein securing the secret in the secure location different from the ROM comprises securing the secret in the secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data stored in the ROM using the secret comprises retrieving at least a portion of the BIOS data stored in the BIOS ROM using the secret.

70. The computer readable program storage device of claim 68, wherein reading the secret from the ROM comprises reading the secret from within the data stored within the ROM.

71. The computer readable program storage device of claim 66, the method further comprising:

reading code from the first location, wherein the code is different from the secret and different from the data stored in the first location;

wherein retrieving at least a portion of the data stored in the first location using the secret comprises retrieving at least a portion of the data stored in the first location using the code and the secret.

72. The computer readable program storage device of claim 71, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory; and

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret.

73. The computer readable program storage device of claim 72, wherein reading the secret within the memory and reading code from the memory further comprises reading the secret from inside the code within the memory.

74. The computer readable program storage device of claim 71, the method further comprising:

unlocking a lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

75. The computer readable program storage device of claim 74, wherein the location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret; and

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

76. The computer readable program storage device of claim 74, the method further comprising:

processing the secret using the code;

wherein unlocking a lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the first location in response to processing the secret using the code.

77. The computer readable program storage device of claim 76, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading code from the first location comprises reading code from the memory, wherein the code is different from the secret and different from the data stored in the memory;

wherein retrieving at least the portion of the data stored in the first location using the code and the secret comprises retrieving at least a portion of the data stored in the memory using the code and the secret;

wherein unlocking the lock bit associated with the data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking the lock bit associated with the data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking the lock bit associated with the data stored in the first location comprises unlocking the lock bit associated with the data stored in the memory in response to processing the secret using the code.

78. The computer readable program storage device of claim 66, the method further comprising:

unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret.

79. The computer readable program storage device of claim 78, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein unlocking a lock bit associated with data stored in the first location prior to retrieving at least the portion of the data stored in the first location using the secret comprises unlocking a lock bit associated with data stored in the memory prior to retrieving at least the portion of the data stored in the memory using the secret.

80. The computer readable program storage device of claim 66, further comprising:

storing the secret within the first location securely;

storing data within the first location securely; and

storing code different from the secret and different from the data within the first location securely.

81. The computer readable program storage device of claim 80, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein storing the secret within the first location securely comprises storing the secret within the memory securely;

wherein storing data within the first location securely comprises storing data within the memory securely; and

wherein storing code different from the secret and different from the data within the first location securely comprises storing code different from the secret and different from the data within the memory securely

82. The computer readable program storage device of claim 81, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM;

wherein storing data within the memory comprises storing data within the ROM;

wherein storing code different from the secret and different from the data within the memory comprises storing code different within secret and different from the data within the ROM;

wherein securing the secret in a secure location different from the memory comprises securing the secret in a secure location different from the ROM; and

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the ROM using the secret.

83. The computer readable program storage device of claim 82, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing data within the ROM comprises storing data within the BIOS ROM;

wherein storing code different within secret and different from the data within the ROM comprises storing code different within secret and different from the BIOS data within the BIOS ROM;

wherein securing the secret in a secure location different from the ROM comprises securing the secret in a secure location different from the BIOS ROM; and

wherein retrieving at least a portion of the data from the ROM using the secret comprises retrieving at least a portion of the BIOS data from the BIOS ROM using the secret.

84. The computer readable program storage device of claim 81, wherein storing a secret within the memory and storing data within the memory comprises storing the secret inside the data within the memory.

85. The computer readable program storage device of claim 81, wherein storing a secret within the memory and storing code different from the secret and different from the data within the memory comprises storing the secret inside the code within the memory.

86. The computer readable program storage device of claim 81, further comprising:

unlocking a lock bit associated with the data prior to retrieving at least the portion of the data from the memory using the secret.

87. The computer readable program storage device of claim 86, further comprising:

reading the code from the memory; and

securing the code in a secure location different from the memory;

wherein retrieving at least a portion of the data from the memory using the secret comprises retrieving at least a portion of the data from the memory using the code and the secret.

88. The computer readable program storage device of claim 87, wherein reading the secret from the memory comprises reading the secret from the memory during a boot sequence; and

wherein securing the secret in a secure location different from the memory comprises storing the secret in SMM memory space.

89. The computer readable program storage device of claim 87, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

processing the code; and

transmitting at least an indication of the secret to the memory;

90. The computer readable program storage device of claim 89, wherein retrieving at least a portion of the data from the memory using the code and the secret further comprises:

receiving a challenge from the memory; and

transmitting a response to the memory including at least an indication of the secret to the memory, in response to receiving the challenge.

91. The computer readable program storage device of claim 66, further comprising:

reading the code from the first location; and

securing the code in a secure location different from the first location;

wherein retrieving at least a portion of the data from the first location using the secret comprises retrieving at least a portion of the data from the first location using the code and the secret.

92. The computer readable program storage device of claim 91, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret;

wherein reading the code from the reading the code from the memory comprises reading the code from the memory;

wherein securing the code in a secure location different from the first location comprises securing the code in a secure location different from the memory; and

wherein retrieving at least a portion of the data from the first location using the secret further comprises retrieving at least a portion of the data from the memory using the code and the secret.

93. The computer readable program storage device of claim 66, wherein reading the secret from the first location comprises reading the secret from the first location during a boot sequence; and

wherein securing the secret in a secure location different from the first location comprises storing the secret in SMM memory space.

94. The computer readable program storage device of claim 93, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from a memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein reading the secret from the memory further comprises reading the secret from the memory during a boot sequence.

95. The computer readable program storage device of claim 66, further comprising:

providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured.

96. The computer readable program storage device of claim 95, wherein the first location comprises a memory;

wherein reading the secret from the first location comprises reading the secret from the memory;

wherein securing the secret in the secure location different from the first location comprises securing the secret in the secure location different from the memory;

wherein retrieving at least the portion of the data stored in the first location using the secret comprises retrieving at least the portion of the data stored in the memory using the secret; and

wherein providing the lock bit associated with the data that when set provides an indication that the data stored in the first location is secured comprises providing a lock bit associated with the data that when set provides an indication that the data stored in the memory is secured

97. A computer readable program storage device encoded with instructions that, when executed by a personal computer system, performs a method of securing data in the personal computer system, the method comprising:

storing a secret within a first location; and

storing code different from the secret within the first location;

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret.

98. The computer readable program storage device of claim 97, wherein the first location comprises a memory;

wherein storing the secret within the first location comprises storing a secret within the memory;

wherein storing code different from the secret within the first location comprises storing code different from the secret within the memory; and

wherein the code is configured to provide access to data stored in the first location when processed in association with the secret further comprises the code being configured to

provide access to data stored in the memory when processed in association with the secret.

99. The computer readable program storage device of claim 98, wherein the memory is a read-only memory (ROM);

wherein storing a secret within the memory comprises storing a secret within the ROM; and

wherein storing code different from the secret within the memory comprises storing code different within secret within the ROM; and

wherein the code is configured to provide access to data stored in the ROM when processed in association with the secret.

100. The computer readable program storage device of claim 99, wherein the data comprises basic input-output system (BIOS) data and the ROM is a BIOS ROM configured to store the BIOS data;

wherein storing a secret within the ROM comprises storing a secret within the BIOS ROM;

wherein storing code different within secret within the ROM comprises storing code different within secret within the BIOS ROM; and

wherein the code is configured to provide access to BIOS data stored in the BISO ROM when processed in association with the secret.

101. The computer readable program storage device of claim 98, wherein storing a secret within the memory comprises storing the secret inside the data within the memory.

102. The computer readable program storage device of claim 98, wherein storing a secret within the memory and storing code different from the secret within the memory comprises storing the secret inside the code within the memory.

103. The computer readable program storage device of claim 98, further comprising: providing a lock bit associated with the data stored in the memory that when set provides an indication that the data stored in the memory is secured.